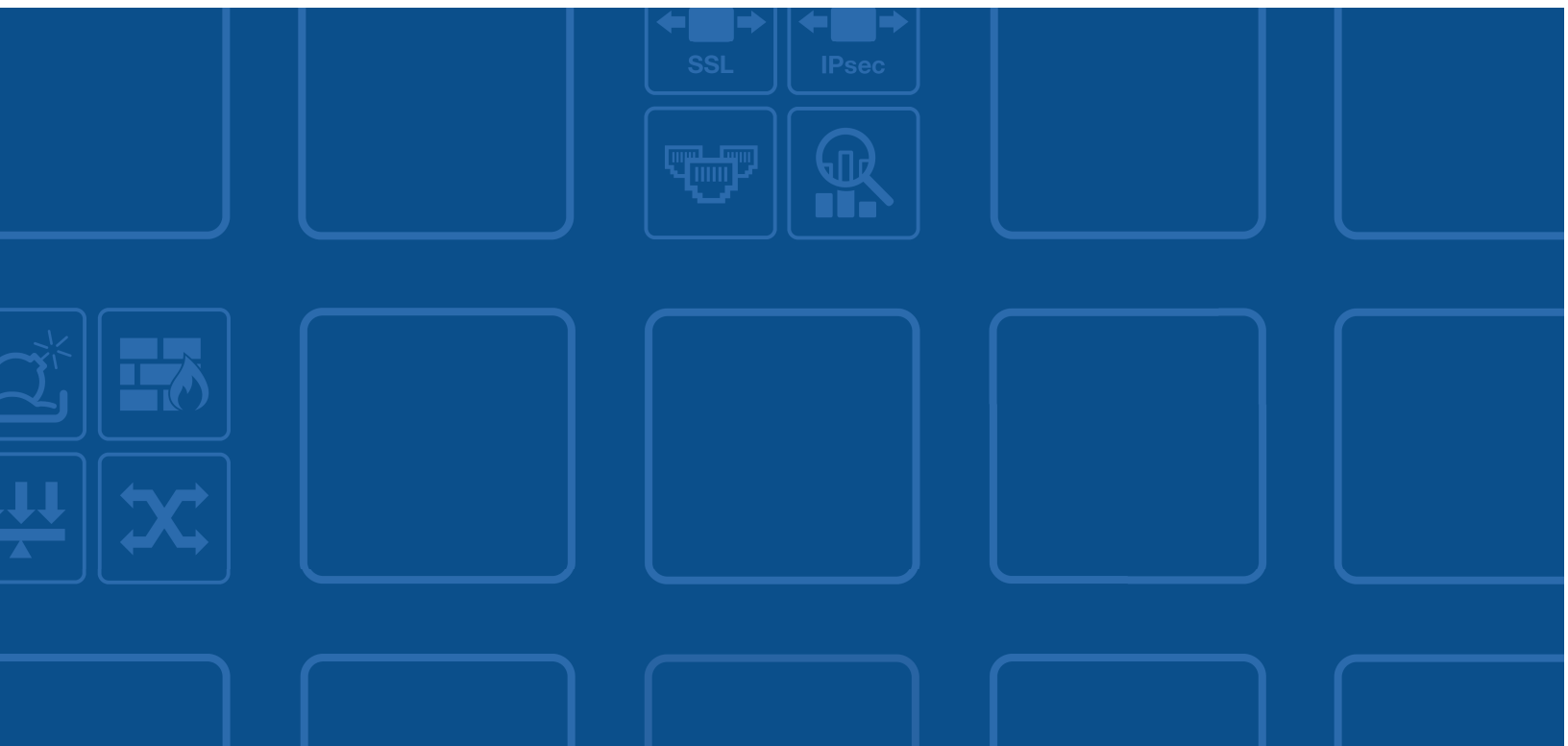
FORTINET
High Performance Network Security

FortiOS - Release Notes

VERSION 5.2.7



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

March 22, 2017

FortiOS 5.2.7 Release Notes

01-527-365075-20170322

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-03-28	Initial release.
2016-04-21	Updated 307923 in Resolved Issues List. Added 307393 to Resolved Issues List.
2016-04-27	Added 355160 to Resolved Issues List.
2016-06-02	Added Microsoft Windows 10 to SSL VPN support.
2016-06-20	Updated the Product Integration & Support. For more details about FortiManager and FortiAnalyzer compatibility with FortiOS, refer the to the FortiManager and FortiAnalyzer Compatibility document available on the Fortinet Document Library.
2016-09-14	Added *Special Notices* > *Removed Local Report Customization* section.
2017-03-22	Removed *273910* from *Known Issues*.

Introduction

This document provides the following information for FortiOS 5.2.7 build 0718:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.2.7 supports the following models.

FortiGate	FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-SFP, FG-60C-POE, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG- 111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-310B-DC, FG-311B, FG-400D, FG-500D, FG-620B, FG-620B-DC, FG- 621B, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-3950B, FG-3951B, FG-5001B, FG-5001C, FG-5001D, FG-5101C
FortiWiFi	FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-60D, FGR-100C
FortiGate VM	FG-VM64, FGT-VM64-AWS/AWSONDEMAND, FG-VM64-AZURE, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B
FortiOS Carrier	FCR-3950B and FCR-5001B FortiOS Carrier 5.2.7 images are delivered upon request and are not available on the customer support firmware download page. FortiOS Carrier firmware image file names begin with *FK*.

The following models are released on a special branch based off of FortiOS 5.2.7. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays the build number.

FGT-5001B/C/D, FGT-5101C	Released on build 8982.
FGT-VM64-AWS/AWSONDEMAND	Released on build 8984.
FGT-VM64-AZURE	Released on build 5273.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 0718.

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0718-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0718-FORTINET.out image.

Last Release of Software

Due to the device flash size limitations, the following FortiGate models' last release of software will be FortiOS version 5.2.5. It is noted that these devices already have entered into their End-of-Life Cycle. Further details and exact dates can be found on the Fortinet Customer Support portal:

Affected Products:

- FortiGate FG-3016B
- FortiGate FG-3810A
- FortiGate FG-5001A SW & DW
- FortiCarrier FK-3810A
- FortiCarrier FK-5001A SW & DW

Special Notices

Compatibility with FortiOS versions

The following units have a new WiFi module built-in that is not compatible with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FWF-60CX-ADSL	PN: 8918-04 and later

The following units have a memory compatibility issue with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FG-600C	PN: 8908-08 and later
FG-600C-DC	PN: 10743-08 and later
FG-600C-LENC	PN: 11317-07 and later

Removed WANOPT, NETSCAN, FEXP features from USB-A

The following features have been removed from the FortiGate and FortiWiFi 80C, 80CM, and 81CM:

- WAN Optimization
- Vulnerability scanning
- Using FortiExplorer on a smartphone to manage the device by connecting to the USB-A port

Removed Local Report Customization

Local report customization has been removed from FortiOS v5.2. You can still record and view local reports, but you can no longer customize their appearance. For more control over customizing local reports, you can use FortiAnalyzer or FortiCloud.

Router Prefix Sanity Check

Prior to FortiOS 5.2.4 under the config router prefix table, if there are any `le` and `ge` settings that have the same prefix length as the prefix, you may lose the prefix rule after upgrading to FortiOS 5.2.4 or later.

WAN Optimization in FortiOS 5.2.4

In FortiOS 5.2.4:

- If your FortiGate does not have a hard disk, WAN Optimization is not available.
- If your FortiGate has a hard disk, you can configure WAN Optimization from the CLI.
- If your FortiGate has two hard disks, you can configure WAN Optimization from the GUI.

See the FortiOS 5.2.4 Feature Platform Matrix to check the availability for your FortiGate model.

Built-In Certificate

FortiGate and FortiWiFi D-series and above have a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate-92D High Availability in Interface Mode

The FortiGate-92D may fail to form an HA cluster and experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used has the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

Default log setting change

For FG-5000 blades and FG-3900 series, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports SATA disk, log disk is enabled by default.

FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from version 5.0.7 (B4625) to FortiOS version 5.2.3, you may experience a back-plane interface connection issue. This is due to a change to

the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

FortiGate units running 5.2.7

FortiGate units running 5.2.7 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

Firewall services

Downgrading from 5.2.3 to 5.2.2 may cause the default protocol number in the firewall services to change. Double check your configuration after downgrading to 5.2.2.

FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

Upgrade Information

Upgrading from FortiOS 5.2.5 or later

FortiOS version 5.2.7 officially supports upgrade from version 5.2.5 or later.

Upgrading from FortiOS 5.0.12 or later

FortiOS version 5.2.7 officially supports upgrade from version 5.0.12 or later.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.2 Supported Upgrade Paths

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.2.7 support

The following table lists 5.2.7 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 42 • Google Chrome version 46 • Apple Safari version 7.0 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Internet Explorer versions 8, 9, 10, and 11 • Mozilla Firefox version 27 • Apple Safari version 6.0 (For Mac OS X) • Google Chrome version 34 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	For the latest information, see the FortiManager and FortiOS Compatibility. You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	For the latest information, see the FortiAnalyzer and FortiOS Compatibility. You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.2.5 and later
FortiClient iOS	• 5.2.2 and later
FortiClient Android and FortiClient VPN Android	• 5.2.7 and later

FortiAP	• 5.2.5 and later • 5.0.10 You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.
FortiSwitch OS (FortiLink support)	• 3.3.0 and later Supported models: FSR112D-POE, FS108D-POE, FS224D-POE, FS124D, FS124D-POE, FS224D-FPOE • 3.2.0 and later Supported models: FS-108D-POE, FS-224D-POE, FSR-112D-POE • 3.0.1 and later Supported model: FS-224D-POE • 2.0.3 Supported models: FS-28C, FS-324B-POE, FS-348B, FS-448B
FortiSwitch-ATCA	• 5.0.3 and later Supported models: FS-5003A, FS-5003B
FortiController	• 5.2.0 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 2.1.0 • 1.4.0 and later • 1.3.0

Fortinet Single Sign-On (FSSO)	• 5.0 build 0247 (needed for FSSO agent support OU in group filters)
	  • Windows Server 2008 (64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	• 4.3 build 0164 (contact Support for download)
	  • Windows Server 2003 R2 (32-bit and 64-bit)
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard Edition
	  • Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExplorer	• 2.6 build 1083 and later. Some FortiGate models may be supported on specific FortiExplorer versions.
FortiExplorer iOS	• 1.0.6 build 0130 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 2.0.0 build 0003 • 1.0.0 build 0024
AV Engine	• 5.174
IPS Engine	• 3.164
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, and 2012 R2
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish (Spain)	✓

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Microsoft Windows XP SP3 (32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2327
Microsoft Windows 10 (32 bit & 64 bit)	2329
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2327

Operating System	Installer
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2327

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit)	Microsoft Internet Explorer versions 9, 10 and 11 Mozilla Firefox version 33
Microsoft Windows 7 SP1 (64-bit)	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Microsoft Windows 8/8.1 (32bit/62bit)	Microsoft Internet Explorer versions 10 and 11 Mozilla Firefox 42
Mac OS 10.9	Safari 7
Linux CentOS version 5.6	Mozilla Firefox version 5.6
Linux Ubuntu version 12.0.4	Mozilla Firefox version 5.6

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✓	✓
Kaspersky Antivirus 2009	✓	
McAfee Security Center 8.1	✓	✓
Trend Micro Internet Security Pro	✓	✓
F-Secure Internet Security 2009	✓	✓

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✓	✓
AVG Internet Security 2011		
F-Secure Internet Security 2011	✓	✓
Kaspersky Internet Security 2011	✓	✓
McAfee Internet Security 2011	✓	✓
Norton 360™ Version 4.0	✓	✓
Norton™ Internet Security 2011	✓	✓
Panda Internet Security 2011	✓	✓
Sophos Security Suite	✓	✓
Trend Micro Titanium Internet Security	✓	✓
ZoneAlarm Security Suite	✓	✓
Symantec Endpoint Protection Small Business Edition 12.0	✓	✓

Resolved Issues

The following issues have been fixed in version 5.2.7. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
304533, 306691	URL field of logging should be up to 512 characters.
355971	`wad` stops working when inspecting virus on the server side.

Firewall

Bug ID	Description
294263	Add the `iprange` check when getting service of traffic logs.

FIPS-CC

Bug ID	Description
303712	FIPS test vectors for FOS 5.2 projects.
309828	Removing `entropy-token` does not trigger a console/log message.
364367	FGT asks for `entropy-token` regardless of the `entropy-token` settings.

FortiCarrier

Bug ID	Description
307176	Due to an out-of-date 3GPP document being used, FortiCarrier drops some GTP packets which should not be dropped.

FortiGate-80C Series

Bug ID	Description
356154	Remove WANOPT,NETSCAN, FEXP from USB-A in FG-80C series (FGT80C/FGT80CM/FWF80CM/FWF81CM).

FortiGate-5001D

Bug ID	Description
306937	System stops working after `set optimize throughput` under `config system global`.

High Availability

Bug ID	Description
302687	`ha-mgmt-interface` IP address is not assigned after reboot.
307013	`hasync` crash signal 11 (FGSP) in `stand-alone-config-sync`.
307413	`standalone-config-sync` is not working as expected.
293314	`standalone-config-sync` units show same expiry date for contracts.
307323	After a failover, SSID was not broadcasted correctly by FWF local-radio.
310721	Failover occurs during Firmware upgrade; it takes approximately 20 seconds.
356239	HA heartbeat is down when restoring a VDOM `config` file.

IPS

Bug ID	Description
305886	Upgrade IPS engine to 3.164.
306461	Change the memory threshold to be 95% usage to enter *conserve mode*.
307443	Fragment IPv6 packet triggered a bad IP header log.

SSL VPN

Bug ID	Description
291674	Delay in accessing internally hosted Sharepoint application via web mode SSL VPN.
290869	SSL VPN `.xls` attachments downloaded from bookmark page are corrupted
293600	Ipv6 SSL VPN pool does not assign `ipv6` address from `iprange`.
301160	Web application does not load when using SSL VPN web access.
307012	SSL VPN is unable to connect in tunnel mode.
356587	SSL VPN portal tablesize is not correct.

System

Bug ID	Description
286229	DNS source IP address settings are ignored.
301702	Fragmented packets are not forwarded in transparent mode.
310686	Admin status down on 40G interface.
246417	The FortiGate unit may become unresponsive and fail to process traffic.
270315	`npu_vlink` connecting NAT and TP VDOMs does not work if HA is enabled.
276628	On NP6 platforms, `npu-vlinks` stops working when adding a transparent VDOM.
295807	FG-1500D master stops working due to FortiCron crash.
300588	Cannot connect SSH to FGT with kex algorithm order `dh-group1-sha1`, `dh-group14-sha1` and `dh-group-exchange-sha1`.
301244	Incoming PPPoE frame is accepted even when the destination MAC address is not local.
308087	High CPU usage when using `session-sync daemon`.
307393	Switch initialization on FGT-3700D is two times. It may stop responding during the second initialization if the shutdown of the first initialization does not work.
355160	FGT800C/1000C system freezes with no response to NMI after upgrading from 5.2.4 to 5.2.5.

User

Bug ID	Description
305484	Increase LDAP filter string size.

Visibility

Bug ID	Description
287164	Restore ability to re-validate dirty sessions against device based policy.

Vulnerability

Bug ID	Description
304861	SSH connection is week when MAC Algorithms are enabled.
307923	Upgrade OpenSSL to 1.0.2g.

WANopt & Webproxy

Bug ID	Description
299764	Increase number of long duration TCP sessions with WANopt enabled.
292174	Crashlog appears when stress testing WANopt and webcache together; the server randomly disconnects.
308409	`wad` stops working.
309945	Poxyworker stops working on incorrect reconnect.
310931	There is no full URL path in the auth-login page.

WiFi

Bug ID	Description
276380	SSID interface MAC address starting with `00:ff` does not act as a WiFi client to take over the gateway IP address.
301853	`Acct-Input/Ouput` attributes are missing in Stop accounting message if `radius-server` are in the non-root VDOM.
305472	Activation of UNII-1 and 3 Band channels for all FAP 11ac models or newer in Korea.
306827	Windows XP clients can now associate FAP with local user group or remote Radius server SSID authentication.
309913	Channel 36,40,44,48 should not be available on FWF local-radio with Region-K.

Known Issues

The following issues have been identified in version 5.2.7. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FortiGate 3810D

Bug ID	Description
285429	Traffic may not be able to go through the NPU VDOM link with traffic sharper enabled on FortiGate-3810D TP mode.

FortiGate-VM

Bug ID	Description
272438	During the boot-up sequence, the FortiGate-VM device may encounter a harmless configuration error message.

FortiSandbox

Bug ID	Description
269830	The UTM log may incorrectly report a file that has been sent to FortiSandbox. *FortiView* > *FortiSandbox* may still show files are submitted even after the daily upload quota has been reached.
273244	On the FortiGate device in *FortiView* > *FortiSandbox*, the analysis result may show a pending status and the FortiCloud side may show an unknown status.

GUI

Bug ID	Description
215890	Local-category status display may not change after running `unset category-override` in the CLI.
246546	Adding an override application signature may cause all category settings to be lost.
267957	The Top Interfering APs chart in the 5G Radio Spectrum Analysis Window may be empty.
268346	*All sessions: filter application*, *threat*, and *threat type*, may not work as expected
271113	When creating an `id_based policy` with SSL enabled, and the set `gui-multipleutm disable` is applied, an *Entry not found* error message may appear.

Bug ID	Description
278638	Explicit policy may be automatically reset to log security events.
285813	When navigating `FortiView > Application` some security action filters may not work.
286226	Users may not be able to create new address objects from the Firewall Policy.

HA

Bug ID	Description
283697	When a new device joins, the list of devices may not synchronize between master and slave.

System

Bug ID	Description
263864	When the interface is configured with *Auto-Speed*, FG-3240C NP4 Port 1G may stay down after reboot. **Workaround**: Set the interface speed to *1000/Full*.
285520	On NP4 platforms, TCP traffic may not be able to be offloaded in the decryption direction.
285981	Adding more than eight members to `LACP get np6_lacp_add_slave` may result in an error.
302272	Medium type may be shown incorrectly on shared ports.
306321	Interface may be mandatory for configuring the GRE tunnel.

VoIP

Bug ID	Description
272278	SIP calls may be denied when using a combination of SIP ALG, IPS, and AppCtrl.

Webfilter

Bug ID	Description
284661	If the requested URL has port number, the URL filter may not block properly.

WiFi

Bug ID	Description
267904	If the client is connecting to an SSID with WPA-Enterprise and User-group, it may not be able to pass the traffic policy.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open Source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

FORTINET®

High Performance Network Security